BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039794
(43)Date of publication of application : 12.02.1999

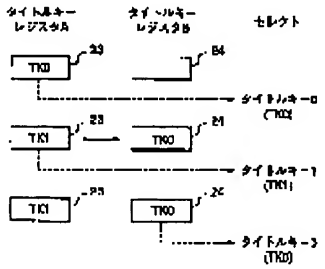
(51)Int.Cl. G11B 20/10

(21)Application number : 09-192785
(22)Date of filing : 17.07.1997

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : KASHIWA HIROSHI

(54) DECIPHERING DEVICE OF CIPHERED DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To quickly decipher ciphered data by deciphering ciphered data in data transmission between two points, i.e., 1 to 1 of an optical disk device recorded with ciphered data in a title key unit to a digital device equipped with a deciphering function of ciphered data, and also many to 1 of plural optical disk devices recorded with ciphered data in the title key unit to the digital device equipped with the deciphering function of ciphered data.
SOLUTION: An authenticating and data deciphering part is provided with plural title key registers A23 and B24, where plural title keys TK0 and TK1 are held respectively When a data deciphering operation of a title 0 is performed again, data deciphering is carried out by selecting the title key register B24 holding the title key TK0 by a CPU without performing authenticating operation and a title key deciphering operation. Consequently, the time required for the authenticating operation to be performed at the time of deciphering the data of the same title key TK0 again is reduced, and hence the ciphered data can quickly be deciphered.



LEGAL STATUS

[Date of request for examination] 17.12.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－39794

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]	識別記号	FI	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ

審査請求　未請求　請求項の数２　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－192785

(22)出願日　平成９年(1997)７月17日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　柏　浩
大阪府門真市大字門真1006番地　松下電器産業株式会社内

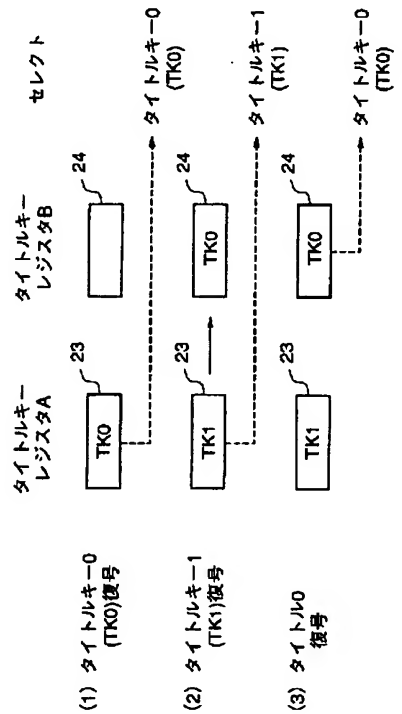
(74)代理人　弁理士　早瀬　憲一

(54)【発明の名称】　暗号データ復号装置

(57)【要約】

【目的】　従来、複数のタイトルキーの暗号データが同一ディスク内に記録されている場合、タイトルキーが変わるごとに認証を行うため、１度復号したタイトルのデータでも認証が必要なため認証時間がかかり効率が悪かったので、この認証時間の短縮化を目的とする。

【解決手段】　認証・データ復号部２に複数のタイトルキーレジスタＡ２３，Ｂ２４を設け、それぞれに複数のタイトルキーＴＫ０，ＴＫ１を保持しておく。再びタイトル０のデータ復号動作を行う場合、認証動作，タイトルキー復号動作を行なうことなくタイトルキーＴＫ０を保持したタイトルキーレジスタＢ２４をＣＰＵ７が選択することでデータ復号を行なう。これにより、再び同じタイトルキーＴＫ０のデータを復号する際に行われる認証動作にかかる時間が削減され、敏速な暗号データの復号を実現できる。



【特許請求の範囲】
【請求項１】　タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク装置とディジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、
上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのＣＰＵデータを生成するＣＰＵと、
上記光ディスク装置の暗号データを復号化する認証・データ復号部と、
上記認証・データ復号部によって復号化されたディジタルデータを記憶するメモリー手段とを備え、
上記認証・データ復号部は、
上記ＣＰＵまたは上記光ディスク装置からのＣＰＵデータを復号処理する暗号・復号アルゴリズムと、
上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための１バイト以上の固定値の鍵である認証キー１を保持する認証キー１レジスタと、
上記認証ごとに変化する１バイト以上の鍵である認証キー２を保持する認証キー２レジスタと、
上記認証ごとに変化する１バイト以上の鍵である認証キー３を保持する認証キー３レジスタと、
上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、
上記暗号・復号アルゴリズムにより生成される異なる１バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、
上記暗号・復号アルゴリズムにおける鍵として上記認証キー１，上記認証キー２，上記認証キー３，上記タイトルキー復号キー，上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とする暗号データ復号装置。
【請求項２】　タイトル単位でタイトルキーの異なる暗号データを複数記録した複数の光ディスク装置とディジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、
上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのＣＰＵデータを生成するＣＰＵと、
上記光ディスク装置の暗号データを復号化する認証・データ復号部と、
上記認証・データ復号部によって復号化されたディジタルデータを記憶するメモリー手段とを備え、
上記認証・データ復号部は、
上記ＣＰＵまたは上記光ディスク装置からのＣＰＵデータを復号処理する暗号・復号アルゴリズムと、
上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための１バイト以上の固定値の鍵である認証キー１を保持する認証キー１レジスタと、
上記認証ごとに変化する１バイト以上の鍵である認証キー２を保持する認証キー２レジスタと、
上記認証ごとに変化する１バイト以上の鍵である認証キー３を保持する認証キー３レジスタと、
上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、
上記複数の光ディスク装置から伝送される暗号データを復号するために各光ディスク装置のそれぞれに対応し、かつ、上記暗号・復号アルゴリズムにより生成される異なる１バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、
上記暗号・復号アルゴリズムにおける鍵として上記認証キー１，上記認証キー２，上記認証キー３，上記タイトルキー復号キー，上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とする暗号データ復号装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、２つのディジタル機器間の伝送または複数のディジタル機器の伝送においてタイトルと呼ばれる単位ごとに暗号化の鍵が異なり、かつタイトルが異なるごとに行う認証の時間短縮を実現する暗号データ復号装置に関するものである。
【０００２】
【従来の技術】図１は、光ディスク装置とディジタルインターフェイスを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図である。図１において、１は光ディスク装置、２は光ディスク装置側の認証部、３は光ディスク装置側のＣＰＵ、４は光ディスク、５は光ディスク装置側のインターフェース回路、６は暗号データ復号装置、７は暗号データ復号装置側のＣＰＵ、８は認証・データ復号部、９は暗号データ復号装置側のインターフェース回路、１０はメモリー回路である。
【０００３】暗号データ復号装置６は、タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク装置１とディジタルインターフェース手段５，９を用いたデータ伝送が行われ、かつ上記光ディスク装置１の暗号データを復号化するものである。この暗号データ復号装置６は、上記光ディスク装置１の暗号データを復号する際に通信主体の認証動作を行うためにＣＰＵデータを生成するＣＰＵ７と、上記光ディスク装置１の暗号データを復号化する認証・データ復号部８と、上記光ディスク装置１とのデータ伝送を行うためのインターフェイス回路９と、上記認証・データ復号部８によって復号

化されたデータを記憶するメモリー回路１０とを備えたものである。

【０００４】上記光ディスク装置１は、光ディスク４に記録された暗号データの認証を行う認証部２と、通信主体の認証動作を行うためにＣＰＵデータを生成するＣＰＵ３と、タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク４と、上記暗号データ復号装置６とのデータ伝送を行うためのインターフェイス回路５とを備えたものである。

【０００５】図６は、従来の暗号データ復号装置６における認証・データ復号部８の構成を示すブロック図である。図６において、１１はデータセレクタ回路、１２はタイトルキー復号のデータを保持するレジスタＣ、１３は認証キー１レジスタ、１４は認証キー２レジスタ、１５は認証キー３レジスタ、１６はタイトルキー復号キーレジスタ、１７はタイトルキーレジスタ、１８はキーセレクタ回路、１９は暗号・復号アルゴリズム（ＤＥＳ：特開昭５１－１０８７０１号公報、特開昭５１－１０８７０２号公報参照。）、２０は認証データを保持するレジスタＡ、２１はコンパレータ回路、２２は認証データを保持するレジスタＢである。

【０００６】以上のように構成された暗号データ復号装置６について、以下にその動作を説明する。なお、光ディスク装置１における認証部２の認証動作は、認証・データ復号部８と同じとする。上記光ディスク装置１のデータをインターフェース回路５を用いて外部の暗号データ復号装置６で復号するためには、認証動作、タイトルキー復号動作、データ復号動作の順に行なう。

【０００７】上記認証動作は、以下のステップ１～ステップ４の手順で行なう。まず、ステップ１として、暗号データ復号装置６のＣＰＵ７より発生した乱数Ｉを、認証・データ復号部８と、インターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２とに伝送する。認証・データ復号部８では、図６に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数Ｉをデータとして選択し、かつ、キーセレクタ回路１８において認証キー１を鍵として選択し、暗号・復号アルゴリズム１９による復号動作を行いその結果Ｉ（認証キー２）を認証キー２レジスタ１４に保持する。また、光ディスク装置１の認証部２においても上記乱数Ｉをデータおよび認証キー１を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより認証キー２を生成する。

【０００８】ステップ２として、光ディスク装置１のＣＰＵ３より発生した乱数IIを、認証部２と、インターフェース回路５により暗号データ復号装置６のＣＰＵ７を介して認証・データ復号部８とに伝送する。認証・データ復号部８では、図６に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数IIをデータとして選択し、かつ、キーセレクタ回路１８において認証キー２レジスタ１４を鍵として選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果II（認証キー３）を認証キー３レジスタ１５に保持する。そして、光ディスク装置１の認証部２においても上記乱数IIをデータおよび認証キー２を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより認証キー３を生成する。

【０００９】ステップ３として、暗号データ復号装置６のＣＰＵ７より発生した乱数III を、認証・データ復号部８と、インターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２とに伝送する。認証・データ復号部８では、図６に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数III をデータとして選択し、かつ、キーセレクタ回路１８において認証キー３レジスタ１５を鍵として選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果III をインターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２に伝送する。そして、光ディスク装置１の認証部２において上記乱数III をデータおよび認証キー３を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより生成された結果IVと、上記結果III の比較結果をＣＰＵ３に送り一致すれば光ディスク装置１における認証が成立する。

【００１０】ステップ４として、光ディスク装置１のＣＰＵ３より発生した乱数IVを、認証部２と、インタフェース回路５により暗号データ復号装置６のＣＰＵ７を介して認証・データ復号部８とに伝送する。そして、認証部２において上記乱数IVをデータとして認証キー３レジスタ１５と同じデータを鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより生成された結果Ｖを、インターフェース回路５によりＣＰＵ７を介して認証・データ復号部８に伝送し、その結果Ｖをレジスタ２０に保持する。認証・データ復号部８では、図６に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数IVをデータとして選択し、かつ、キーセレクタ回路１８において認証キー３レジスタ１４を鍵として選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果VIをレジスタＢ２２に保持する。そして、コンパレータ回路２１において上記レジスタＡ２０に保持した結果Ｖと、上記レジスタＢ２２に保持した結果VIとの比較結果をＣＰＵ７に送り一致すれば暗号データ復号装置６における認証が成立する。

【００１１】このようにして、相互の認証が成立した所で、次のタイトルキー復号動作を行なうこととなる。タイトルキーは、タイトルキー復号キーを鍵として暗号・復号アルゴリズムを用いて暗号化して光ディスク４に記録している。したがって、例えば、タイトルキーＡの復号は光ディスク４における再生したいタイトルＡのタイトルキーＡを、ＣＰＵ３を介して認証部２へ送り、そのタイトルキーＡをデータとして、認証キー２レジスタ１

４を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより暗号化し、その結果であるタイトルキーＡをインターフェース回路５により暗号データ復号装置６へ伝送する。暗号データ復号装置６では、図６に示すように、伝送された上記タイトルキーＡと認証キー２より暗号・復号アルゴリズム１９を用いて復号動作を行いその結果をレジスタＣ１２に保持する。次に、データセレクタ回路１１においてレジスタＣ１２を選択し、かつ、キーセレクタ１８においてタイトルキー復号キー１６を選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果であるタイトルキーＡをタイトルキーレジスタ１７に保持する。

【００１２】上記タイトルキーの復号が終了した後に、以下のデータ復号動作を行なう。光ディスク４のデータは、タイトル単位でタイトルキーを鍵として暗号・復号アルゴリズムにより暗号化している。したがって、データの復号は光ディスク４より再生したいタイトルのデータをインターフェース回路５により暗号データ復号装置６の認証・データ復号部８に伝送する。認証・データ復号部８では、図６に示すように、データセレクタ回路１１においてインターフェース回路９からのデータを選択し、かつ、キーセレクタ回路１８においてタイトルキーレジスタ１７を鍵として選択し、暗号・復号アルゴリズム１９による復号動作を行い、ここで復号化されたデータはメモリー回路１０に保持される。

【００１３】以上のようにして、タイトルが変わるごとに上記認証動作、上記タイトルキー復号動作、上記データ復号動作を順次行なうことになる。

【００１４】

【発明が解決しようとする課題】しかしながら、上記の従来の暗号データ復号装置の構成では、複数のタイトルキーで暗号化したデータが同一ディスク内に記録されている場合においてタイトルキーが変わるごとに認証を行うため、１度復号したタイトルキーに戻って暗号データを復号したい時も認証が必要なため認証時間がかかり効率が悪いということで問題点を有していた。

【００１５】本発明は、上記従来の問題点を解決するためになされたものであり、要するに複数のタイトルキーを保持するレジスタを設けることにより、タイトルキー単位で暗号データが記録されている光ディスク装置と暗号データの復号機能を備えたディジタル装置の１対１，つまり２点間のデータ伝送における暗号データの復号化、およびタイトルキー単位で暗号データが記録されている複数の光ディスク装置と暗号データの復号機能を備えたディジタル装置の複数対１のデータ伝送における暗号データの復号化を敏速に行う暗号データ復号装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の請求項１に係る暗号データ復号装置は、タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク装置とディジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのＣＰＵデータを生成するＣＰＵと、上記光ディスク装置の暗号データを復号化する認証・データ復号部と、上記認証・データ復号部によって復号化されたデータを記憶するメモリー手段とを備え、上記認証・データ復号部は、上記ＣＰＵまたは上記光ディスク装置からのＣＰＵデータを復号処理する暗号・復号アルゴリズムと、上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する，認証を行うための１バイト以上の固定値の鍵である認証キー１を保持する認証キー１レジスタと、上記認証ごとに変化する１バイト以上の鍵である認証キー２を保持する認証キー２レジスタと、上記認証ごとに変化する１バイト以上の鍵である認証キー３を保持する認証キー３レジスタと、上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、上記暗号・復号アルゴリズムにより生成される異なる１バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、上記暗号・復号アルゴリズムにおける鍵として上記認証キー１，上記認証キー２，上記認証キー３，上記タイトルキー復号キー，上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とするものである。

【００１７】また、本発明の請求項２に係る暗号データ復号装置は、タイトル単位でタイトルキーの異なる暗号データを複数記録した複数の光ディスク装置とディジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのＣＰＵデータを生成するＣＰＵと、上記光ディスク装置の暗号データを復号化する認証・データ復号部と、上記認証・データ復号部によって復号化されたディジタルデータを記憶するメモリー手段とを備え、上記認証・データ復号部は、上記ＣＰＵまたは上記光ディスク装置からのＣＰＵデータを復号処理する暗号・復号アルゴリズムと、上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための１バイト以上の固定値の鍵である認証キー１を保持する認証キー１レジスタと、上記認証ごとに変化する１バイト以上の鍵である認証キー２を保持する認証キー２レジスタと、上記認証ごとに変化する１バイト以上の鍵である認証キー３を保持する認証キー３レジスタと、上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、上記複数の光ディスク装置から伝送される暗号データを復号するために各光デ

ィスク装置のそれぞれに対応し、かつ、上記暗号・復号アルゴリズムにより生成される異なる１バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、上記暗号・復号アルゴリズムにおける鍵として上記認証キー１，上記認証キー２，上記認証キー３，上記タイトルキー復号キー，上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とするものである。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

実施の形態１．図１は、本発明の実施の形態１による，光ディスク装置とディジタルインターフェイスを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図であり、光ディスク装置１や暗号データ復号装置６のブロック構成は、従来のものと同様である。図２は、本実施の形態１による暗号データ復号装置６における認証・データ復号部８の構成を示すブロック図である。

【００１９】実施の形態１は、光ディスク装置と暗号データ復号装置との１対１，つまり２点間のディジタルインターフェイスを用いたデータ伝送において、タイトル単位で暗号化したデータの円滑な復号化を行える暗号データ復号装置である。すなわち、実施の形態１の暗号データ復号装置６が、図６のブロック図に示した従来のものと異なるところは、従来のものではタイトルキーレジスタ１７が１つしかなかったのに対し、実施の形態１のものでは図２に示すように、タイトルキーレジスタＡ２３とタイトルキーレジスタＢ２４と２つ有することである。

【００２０】図３は、図２に示す如く、タイトルキーレジスタＡ２３とタイトルキーレジスタＢ２４とを２つ備えた場合の上記認証・データ復号部８のデータ復号図である。図３において、２３はタイトルキーレジスタＡ、２４はタイトルキーレジスタＢである。また、ＴＫ０はタイトル０におけるタイトルキー、ＴＫ１はタイトル１におけるタイトルキーである。

【００２１】以上のように構成された暗号データ復号装置について、以下にその動作を説明する。

【００２２】まず、光ディスク装置１のデータをインターフェース回路５を用いて外部の暗号データ復号装置６で復号するには認証動作、タイトルキー復号動作、データ復号動作の順に行なう。

【００２３】上記認証動作は、以下のステップ１～ステップ４の手順で行なう。タイトル０を再生するためには、まず、ステップ１として、暗号データ復号装置６のＣＰＵ７より発生した乱数Ｉを認証・データ復号部８とインターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２とに伝送する。認証・データ復号部８では、図２に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数Ｉをデータとして選択し、かつ、キーセレクタ回路１８において認証キー１を鍵として選択し、暗号・復号アルゴリズム１９による復号動作を行いその結果Ｉを認証キー２レジスタ１４に保持する。また、光ディスク装置１の認証部２においても上記乱数Ｉをデータおよび認証キー１を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより認証キー２を生成する。

【００２４】ステップ２として、光ディスク装置１のＣＰＵ３より発生した乱数IIを認証部２と、インターフェース回路５により暗号データ復号装置６のＣＰＵ７を介して認証・データ復号部８とに伝送する。認証・データ復号部８では、図２に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数IIをデータとして選択し、かつ、キーセレクタ回路１８において認証キー２レジスタ１４を鍵として選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果IIを認証キー３レジスタ１５に保持する。また、光ディスク装置１の認証部２においても上記乱数IIをデータおよび認証キー２を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより認証キー３を生成する。

【００２５】ステップ３として、暗号データ復号装置６のＣＰＵ７より発生した乱数III を認証・データ復号部８と、インターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２とに伝送する。認証・データ復号部８では、図２に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数III をデータとして選択し、かつ、キーセレクタ回路１８において認証キー３レジスタ１５を鍵として選択し、暗号・復号アルゴリズム１９により復号動作を行いその結果III を、インターフェース回路９により光ディスク装置１のＣＰＵ３を介して認証部２に伝送する。また、光ディスク装置１の認証部２において上記乱数IIIをデータおよび認証キー３を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより生成された結果IVと上記結果３の比較結果をＣＰＵ３に送り一致すれば光ディスク装置１における認証が成立する。

【００２６】ステップ４として、光ディスク装置１のＣＰＵ３より発生した乱数IVを認証部２と、インタフェース回路５により暗号データ復号装置６のＣＰＵ７を介して認証・データ復号部８に伝送する。また、認証部２において上記乱数IVをデータとして認証キー３レジスタ１５と同じデータを鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより生成された結果Ｖを、インターフェース回路５によりＣＰＵ７を介して認証・データ復号部８に伝送し、レジスタＡ２０に保持する。認証・データ復号部８では、図２に示すように、データセレクタ回路１１においてＣＰＵデータである上記乱数IVをデータとして選択し、かつ、キーセレクタ回路１８において認証キー３レジスタ１４を鍵として選択し、暗

号・復号アルゴリズム１９により復号動作を行いその結果VIをレジスタＢ２２に保持し、コンパレータ回路２１においてレジスタＡ２０とレジスタＢ２２の比較結果をＣＰＵ７に送り一致すれば暗号データ復号装置６における認証が成立する。このようにして、相互の認証が成立した所で、タイトル０のタイトルキー復号動作を行なうこととなる。

【００２７】タイトルキーＴＫ０は、タイトルキー復号キーを鍵として暗号・復号アルゴリズムを用いて暗号化して光ディスク４に記録している。したがって、タイトルキーＴＫ０の復号は光ディスク４における再生したいタイトル０のタイトルキーＴＫ０をＣＰＵ３を介して認証部２へ送り、タイトルキーＴＫ０をデータとして、認証キー２レジスタ１４を鍵として用いて暗号・復号アルゴリズム１９と同じアルゴリズムにより暗号化した結果であるタイトルキーＴＫ０をインターフェース回路５により暗号データ復号装置６へ伝送する。暗号データ復号装置６では伝送された上記タイトルキーＴＫ０と認証キー２より暗号・復号アルゴリズム１９を用いて復号動作を行いその結果をレジスタＣ１２に保持する。次に、データセレクタ回路１１においてレジスタＣ１２を選択し、かつ、キーセレクタ回路１８においてタイトルキー復号キー１６を選択し、暗号・復号アルゴリズム１９により上記タイトル０のデータの複合に必要なタイトルキーＴＫ０のタイトルキー復号動作を行いその結果を、図３(1) に示すように、タイトルキーレジスタＡ２３に保持する。上記タイトルキーＴＫ０の復号が終了後に、上記タイトル０のデータ復号動作を行なう。

【００２８】光ディスク４のデータは、タイトル単位でタイトルキーを鍵として暗号・復号アルゴリズムにより暗号化している。したがって、タイトル０のデータの復号は光ディスク４より再生したいタイトル０のデータをインターフェース回路５により暗号データ復号装置６の認証・データ復号部８に伝送する。認証・データ復号部８では、図２に示すように、データセレクタ回路１１においてインターフェース回路９からのデータを選択し、かつ、キーセレクタ回路１８においてタイトルキーレジスタＡ２３を鍵として選択し、暗号・復号アルゴリズム１９によりタイトル０のデータの復号動作を行い、そして復号化されたタイトル０のデータはメモリー回路１０に保持される。

【００２９】次に、タイトル１を再生するために、上記認証動作を行い、上記タイトル１のデータの復号に必要なタイトルキーＴＫ１を上記タイトルキー復号動作によりタイトルキーレジスタＡ２３に保持し、上記タイトルキーレジスタＡ２３を鍵として上記データ復号動作により上記タイトル１のデータを復号する。この時、図３(2) に示すように、上記タイトル０のタイトルキーＴＫ０をタイトルキーレジスタＡ２３からタイトルキーレジスタＢ２４に移し保持する。このようにして、順次新しいタイトルキーＴＫ２，ＴＫ３，・・・を復号するごとにタイトルキーレジスタＡ２３に保持すると同時にタイトルキーレジスタＡ２３にあったタイトルキーＴＫ１，ＴＫ２，・・・をタイトルキーレジスタＢ２４に移し保持する。

【００３０】ここで、新たに上記タイトル０のデータ復号動作を行いたい場合は、上記認証動作および上記タイトルキー復号動作を行なうことなく、図３(3) に示すように、上記ＣＰＵ７がタイトルキーレジスタＢ２４を選択することで、タイトル０のデータの復号を行なう。

【００３１】このように、本実施の形態１による暗号データ復号装置６によれば、タイトルキーレジスタＡ２３、タイトルキーレジスタＢ２４を選択することで上記認証動作および上記タイトルキー復号動作を行なうことなく、光ディスク装置１のデータの復号を行なうので、タイトルキー単位で暗号データが記録されている光ディスク装置と暗号データの復号機能を備えたディジタル装置の１対１，つまり２点間のデータ伝送における暗号データの復号化を敏速に行うものが実現できるという効果がある。

【００３２】実施の形態２．図４は、本実施の形態２による暗号データ復号装置６における認証・データ復号部８の構成を示すブロック図である。図５は、図４に示す如く、タイトルキーレジスタＡ２３とタイトルキーレジスタＢ２４とタイトルキーレジスタＣ２５とを３つ備えた場合の上記認証・データ復号部８のデータ復号図である。図５において、２６は光ディスク装置Ａ、２７は光ディスク装置Ｂ、２８は光ディスク装置Ｃ、２３はタイトルキーレジスタＡ、２４はタイトルキーレジスタＢ、２５はタイトルキーレジスタＣである。また、ＴＫＡはタイトルＡにおけるタイトルキー、ＴＫＢはタイトルＢにおけるタイトルキー、ＴＫＣはタイトルＣにおけるタイトルキーである。

【００３３】実施の形態２は、３台の光ディスク装置と暗号データ復号装置との３対１でのディジタルインターフェイスを用いたデータ伝送において、タイトル単位で暗号化したデータの円滑な復号化を行える暗号データ復号装置である。すなわち、実施の形態２による暗号データ復号装置は、図４，図５に示すように、３台の光ディスク装置Ａ，Ｂ，Ｃと暗号データ復号装置６の３対１でのタイトルキーレジスタを３つ（タイトルキーレジスタＡ２３，Ｂ２４，Ｃ２５）備えた場合における上記認証・データ復号部８を有するものである。

【００３４】次に、実施の形態２による暗号データ復号装置６の動作を説明する。まず、光ディスク装置Ａ２６、光ディスク装置Ｂ２７、光ディスク装置Ｃ２８の順にデータの復号を行う。光ディスク装置Ａ２６のタイトルＡを再生するために、上記実施の形態１で説明したときと同様に、上記認証動作を行い上記タイトルＡのデータの復号に必要なタイトルキーＴＫＡを上記タイトルキ

ー復号動作によりタイトルキーレジスタＡ２３に保持し、上記タイトルキーレジスタＡ２３を鍵として上記データ復号動作により上記タイトルＡのデータを復号する。

【００３５】同様に、光ディスク装置Ｂ２７のタイトルＢを再生するために、上記認証動作を行い、上記タイトルＢのデータの復号に必要なタイトルキーＴＫＢを上記タイトルキー復号動作によりタイトルキーレジスタＢ２４に保持し、上記タイトルキーレジスタＡ２４を鍵として上記データ復号動作により上記タイトルＢのデータを復号する。

【００３６】また、光ディスク装置Ｃ２８のタイトルＣを再生するために、上記認証動作を行い、上記タイトルＣのデータの復号に必要なタイトルキーを上記タイトルキー復号動作によりタイトルキーレジスタＣ２５に保持し、上記タイトルキーレジスタＣ２５を鍵として上記データ復号動作により上記タイトルＣのデータを復号する。

【００３７】なお、上記実施の形態１では、図３に示すように、予めタイトルキーレジスタＡ２３にタイトルキーＴＫ０が保持されている場合、次にタイトル１のデータを復号するとき、このタイトルキーＴＫ０をタイトルキーレジスタＢ２４に移していたが、実施の形態２では、３台の光ディスク装置にそれぞれ対応してタイトルキーレジスタが１つずつ設けられているものであるため、このようなタイトルキーの移動は行われない。

【００３８】次に、例えば、光ディスク装置Ｃ２８の上記タイトルＣのデータ復号後に、光ディスク装置Ａ２６の上記タイトルＡを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、ＣＰＵ７がタイトルキーレジスタＡ２３を選択することで上記タイトルＡのデータを復号し、また、光ディスク装置Ｂ２７の上記タイトルＢを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、ＣＰＵ７がタイトルキーレジスタＢ２４を選択することで上記タイトルＢのデータを復号し、さらに、光ディスク装置Ｃ２８の上記タイトルＣを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、ＣＰＵ７がタイトルキーレジスタＣ２５を選択することで上記タイトルＣのデータを復号する。

【００３９】このように、本実施の形態２による暗号データ復号装置によれば、３台の光ディスク装置Ａ２６，Ｂ２７，Ｃ２８のそれぞれの最後にアクセスしたタイトルキーＴＫＡ，ＴＫＢ，ＴＫＣをタイトルキーレジスタＡ２３、タイトルキーレジスタＢ２４、タイトルキーレジスタＣ２５に保持し、タイトルキーレジスタＡ２３、タイトルキーレジスタＢ２４、タイトルキーレジスタＣ２５のいずれかを選択することで上記認証動作および上記タイトルキー復号動作を行なうことなく、光ディスク装置Ａ２６、光ディスク装置Ｂ２７、光ディスク装置Ｃ２８のデータの復号を行なうので、タイトルキー単位で暗号データが記録されている複数の光ディスク装置と暗号データの復号機能を備えたディジタル装置の複数対１のデータ伝送における暗号データの復号化を敏速に行うものを実現できるという効果がある。

【００４０】なお、本発明に係る暗号データ復号装置は、上記実施の形態２のものでは、光ディスク装置Ａ２６，Ｂ２７，Ｃ２８のそれぞれに対応したタイトルキーレジスタが１つずつ設けられているものであるが、この実施の形態２のものにおいて、例えば、上記実施の形態１の如く、光ディスク装置Ａ２６，Ｂ２７，Ｃ２８のそれぞれに対応したタイトルキーレジスタが複数個ずつ設けられているものであってよい。また、実施の形態２では、３台の光ディスク装置との間でディジタルインターフェイスを用いたデータ伝送を行うものであるが、本発明に係る暗号データ復号装置にあっては、任意の複数台の光ディスク装置との間でディジタルインターフェイスを用いたデータ伝送を行うものであってもよい。

【００４１】

【発明の効果】以上のように、本発明の請求項１に係る暗号データ復号装置によれば、暗号・復号アルゴリズムにより生成される異なる１バイト以上のタイトルキーを２つ以上保持するレジスタを備えることにより、タイトルキーと呼ばれる鍵を用いて暗号化したデータを複数記録した光ディスク装置からディジタル伝送される暗号データの復号機能を備えたディジタル装置（暗号データ復号装置）への１対１，つまり２点間のディジタルインターフェースを用いたデータ伝送において、１度復号したタイトルキーに戻って暗号データを復号したい時に認証動作することなく復号でき、これにより、暗号データの復号化を敏速に行えるものが実現できるという効果がある。

【００４２】また、本発明の請求項２に係る暗号データ復号装置によれば、複数の光ディスク装置と暗号データの復号機能を備えたディジタル装置（暗号データ復号装置）の複数対１のデータ伝送において、複数の光ディスク装置のそれぞれがアクセスしたタイトルキーを保持することで再び同じタイトルキーの光ディスク装置のデータを復号する場合に認証動作することなく復号でき、これにより、暗号データの復号化を敏速に行えるものが実現できるという効果がある。

【図面の簡単な説明】

【図１】　実施の形態１，および従来における，光ディスク装置とディジタルインターフェイスを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図である。

【図２】　実施の形態１による暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

【図３】　実施の形態１による暗号データ復号装置の認

証・データ復号部におけるデータ復号図である。

【図４】　実施の形態２による暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

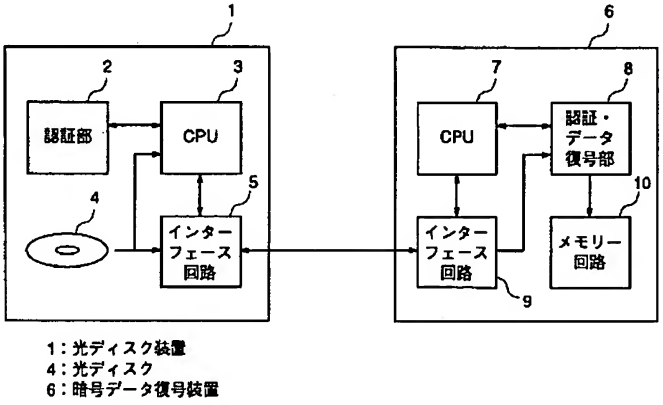
【図５】　実施の形態２による暗号データ復号装置の認証・データ復号部におけるデータ復号図である。

【図６】　従来の暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

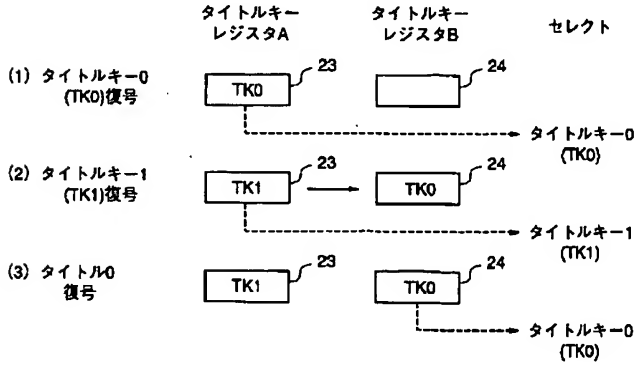
【符号の説明】

１．光ディスク装置
２　認証部
３　ＣＰＵ
４　光ディスク
５　光ディスク装置におけるインターフェース回路
６　暗号データ復号装置
７　ＣＰＵ
８　認証・データ復号部
９　暗号データ復号装置におけるインターフェース回路
１０　メモリー回路
１１　データセレクタ回路
１２　レジスタＣ
１３　認証キー１レジスタ
１４　認証キー２レジスタ
１５　認証キー３レジスタ
１６　タイトルキー復号キーレジスタ
１７　タイトルキーレジスタ
１８　キーセレクタ回路
１９　暗号・復号アルゴリズム
２０　レジスタＡ
２１　コンパレータ回路
２２　レジスタＢ
２３　タイトルキーレジスタＡ
２４　タイトルキーレジスタＢ
２５　タイトルキーレジスタＣ
２６　光ディスク装置Ａ
２７　光ディスク装置Ｂ
２８　光ディスク装置Ｃ

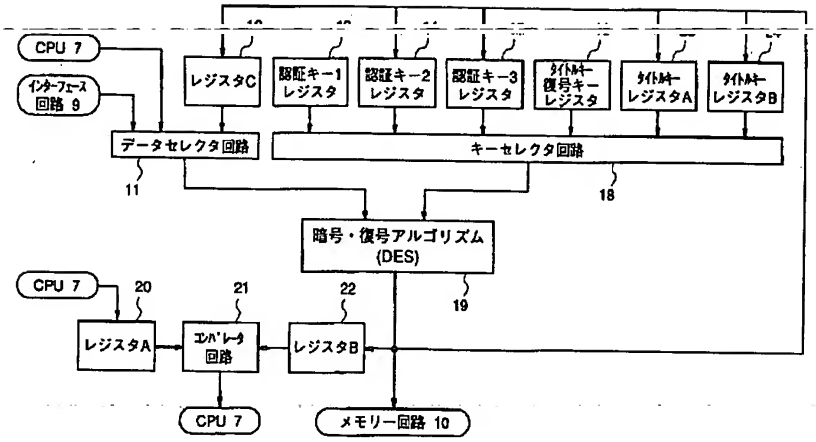
【図１】



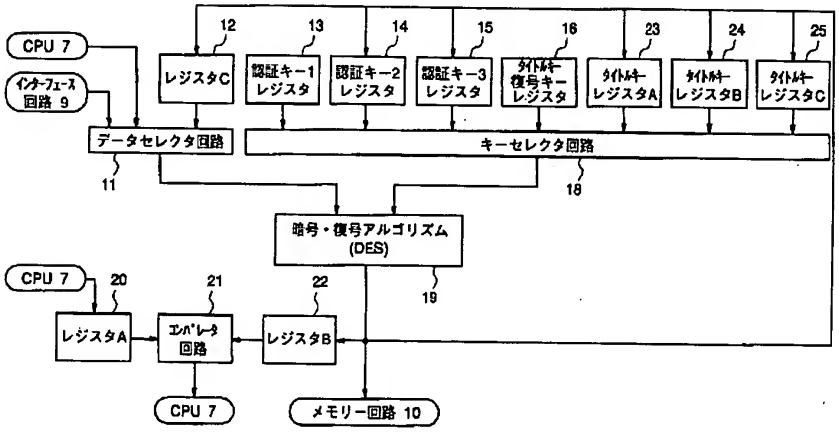
【図３】



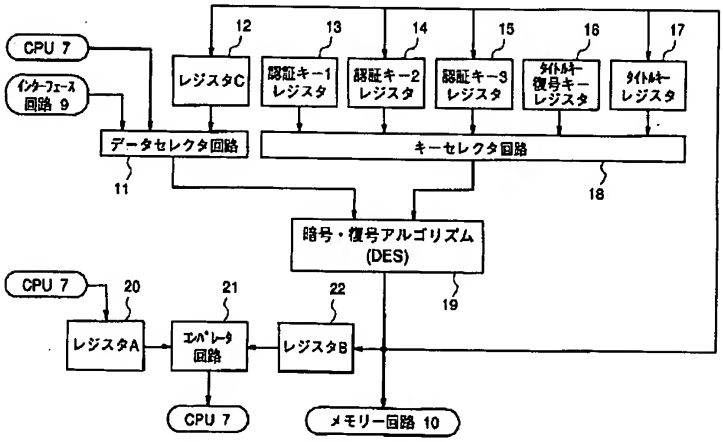
【図２】


CPU 7
インターフェース回路 9
レジスタC
認証キー-1レジスタ
認証キー-2レジスタ
認証キー-3レジスタ
タイトルキー復号キーレジスタ
タイトルキーレジスタA
タイトルキーレジスタB
データセレクタ回路
キーセレクタ回路
11
18
暗号・復号アルゴリズム(DES)
19
CPU 7
20
21
22
レジスタA
エンバレータ回路
レジスタB
CPU 7
メモリー回路 10

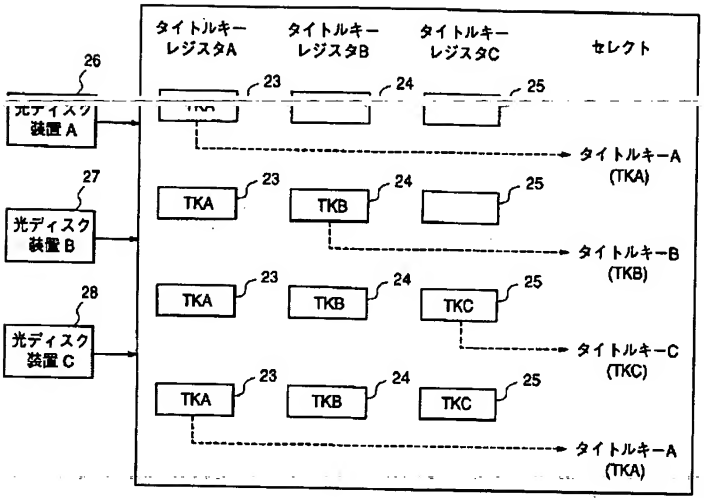
【図４】


CPU 7
インターフェース回路 9
12
13
14
15
16
23
24
25
レジスタC
認証キー-1レジスタ
認証キー-2レジスタ
認証キー-3レジスタ
タイトルキー復号キーレジスタ
タイトルキーレジスタA
タイトルキーレジスタB
タイトルキーレジスタC
データセレクタ回路
キーセレクタ回路
11
18
暗号・復号アルゴリズム(DES)
19
CPU 7
20
21
22
レジスタA
エンバレータ回路
レジスタB
CPU 7
メモリー回路 10

【図６】


CPU 7
インターフェース回路 9
12
13
14
15
16
17
レジスタC
認証キー-1レジスタ
認証キー-2レジスタ
認証キー-3レジスタ
タイトルキー復号キーレジスタ
タイトルキーレジスタ
データセレクタ回路
キーセレクタ回路
11
18
暗号・復号アルゴリズム(DES)
19
CPU 7
20
21
22
レジスタA
エンバレータ回路
レジスタB
CPU 7
メモリー回路 10

【図5】


タイトルキー
レジスタA
タイトルキー
レジスタB
タイトルキー
レジスタC
セレクト
26
23
24
25
光ディスク
装置A
タイトルキーA
(TKA)
27
光ディスク
装置B
TKA
TKB
タイトルキーB
(TKB)
28
光ディスク
装置C
TKC
タイトルキーC
(TKC)
タイトルキーA
(TKA)